

5    The claims

1. A method for a person to sign a document (as defined herein) by use of an electronic pen (as defined herein), including the steps of:

(a) capturing a hand signature (as defined herein) of the person;

10 (b) generating a verification ID; then

(c) attaching the hand signature and the verification ID and an optical watermark to the document to complete the document signing process.

15 2. A method as claimed in claim 1, wherein the identity of the person is verified before generating the verification ID, the verification ID being generated from one or more of the group consisting of: the captured hand signature, a document digest, a time stamp, and representative features of the document.

20 3. A method as claimed in claim 1, wherein the captured hand signature is embedded into the optical watermark.

4. A method as claimed in claim 3, wherein one or more selected from the group consisting of: the document digest and a time stamp, is embedded into the optical watermark to form a link between the document and the hand signature.

25

5. A method as claimed in claim 2, wherein the document digest is critical information of the document.

30 6. A method as claimed in claim 1, wherein the person's identity is verified by a public key infrastructure after a security handshaking challenge-and-response session between a server and the electronic pen.

35 7. A method as claimed in claim 6, wherein the electronic pen stores one or more selected from the group consisting of: an identity number of the electronic pen, a private key of the electronic pen, a private key of the person, measured features of the person's hand signature, and a detachable learning module.

5

8. A method as claimed in claim 7, wherein there is a plurality of persons able to use the electronic pen, the electronic pen being able to store registration information of each such person.

10 9. A method as claimed in claim 7, wherein the server and e-pen store their private keys respectively, and the hand signature and/or measured features of the hand signature of the person are stored in the server.

15 10. A method as claimed in claim 9, wherein there is included a preliminary step of security handshaking between the server and the electronic-pen based on public key pairs.

11. A method as claimed in claim 7, wherein the hand signature and/or measured features of the hand signature of the person are stored in the electronic-pen, and the processing and verification of the hand signature are also carried out in the electronic-pen.

20 12. A method as claimed in claim 7, wherein there is a security authentication process between the server and the electronic-pen, as well as between the server and a service program.

25 13. A method as claimed in claim 12, wherein after successful completion of the security handshaking, the electronic-pen collects hand signature data, encrypts the hand signature data, and sends it to the server for further processing and verification.

30 14. A method as claimed in claim 12 wherein the capturing and processing of the hand signature and/or measured features of the hand signature of the person are carried out in a secure processor.

15. A method as claimed in claim 13, wherein the processing result are sent to the electronic pen for verification.

35 16. A method as claimed in claim 7, wherein the private key and the hand signature of the person are stored in the electronic pen.

5

17. A method as claimed in claim 14, wherein the hand signature and/or the measured features of the hand signature of the person are stored in the secure processor.

10 18. A method as claimed in claim 14, wherein the hand signature and/or the measured features of the hand signature are stored in the server.

15 19. A method as claimed in claim 7, wherein the hand signature and/or the measured features of the hand signature of the person are stored in an encrypted form.

20 20. A method as claimed in claim 7, wherein the hand signature and/or the measured features of the hand signature of the person are stored in a secure memory.

20 21. A method as claimed in claim 20, wherein the secure memory is an authentication card for the person.

25 22. A method as claimed in claim 12, further including a document-handling module in the computer for displaying the document and incorporating the hand signature into the document.

23. A method as claimed in claim 1, further including at least one seal image in the electronic pen so that upon signing the document both the hand signature of the person and the at least one seal image will appear on the document.

30 24. A method as claimed in claim 23, wherein the at least one seal image is an optical watermark in which is embedded hidden information to protect against forgeries.

25. A method as claimed in claim 1, wherein the method is applied to process approval.

35 26. A method for generating a validated hand signature (as defined herein) to a document (as defined herein) including the steps of:

(a) signing the document using an electronic pen (as defined herein);

- 5 (b) creating a digest of the document;  
(c) encrypting the hand signature within the electronic pen;  
(d) generating a verification ID; and  
(e) incorporating the verification ID into the document, and integrating the digest into the document.

10

27. A method as claimed in claim 26, wherein the verification ID is generated from one or more of the group consisting of: the captured hand signature, the document digest, a time stamp, and representative features of the document.

15 28. A method as claimed in claim 26, wherein the hand signature is embedded into an optical watermark.

29. A method as claimed in claim 28, wherein at least one of the document digest, critical features of the document contents, and a time stamp, are embedded into the optical watermark to form a link between the document and the hand signature.

20 30. A method as claimed in claim 29, wherein the document is authenticated by creating a digest of the signed document; generating a decrypt key using the document digest and using it to decrypt the verification ID; comparing the hand signature extracted from the verification ID and the hand signature as it appears on the signed document; and comparing the digest generated from the document and the digest from the verification ID.

25 31. A method as claimed in claim 30, wherein there is included the additional steps of comparing the hand signature on the document with that embedded in the optical watermark; and comparing that of the critical features/content of the document and time stamp embedded in the optical watermark with its equivalent in the document.

30 32. A method as claimed in claim 26, wherein the digest of the document is obtained from the representative features of the document.

35

33. A method as claimed in claim 31, wherein that which is embedded in the optical watermark is decoded by a special key.

5

34. A method as claimed in claim 26, wherein when the document is a printed document, the hand signature and the digest of the document are extracted from the printed document.

10 35. A method as claimed in claim 34, wherein the document authenticity is verified by comparing the hand signature on the document with the hand signature embedded in the optical watermark.

15 36. A method as claimed in claim 35, wherein the critical features/content of the document and the time stamp embedded in the optical watermark are compared with its equivalent in the document.

37. A method as claimed in claim 26, wherein the hand signature and the time stamp are encrypted using an encryption key generated from the digest of the document.

20 38. A method as claimed in claim 37, wherein the digest of the document is used to obtain an encryption key pair from a database of encryption key pairs.

25 39. A method as claimed in claim 37, wherein the document digest is used to generate and encryption key pair using a secret function.

40. A method as claimed in claim 38, wherein the database and the secret function are located in one of the group consisting of: the electronic pen, a server, and a secure memory.

30

41. A method as claimed in claim 1, wherein the hand signature includes signature image and features of the hand signature.

42. A method as claimed in claim 41, wherein the features of the hand signature include pressure and speed.

5 43. A method as claimed in claim 1, wherein pre-registered hand signatures are stored for future use.

44. A method as claimed in claim 43, wherein the pre-registered hand signatures are stored in one or more selected from the group consisting of: the electronic pen, the server, and

10 the secure memory.

45. A method as claimed in claim 43, wherein the pre-registered hand signatures are periodically updated.

15 46. A method as claimed in claim 1, wherein the hand signature is combined with other biometric information of the person.

47. A method as claimed in claim 1, wherein encryption is by one or more selected from the group consisting of: public key pair and symmetry key.